(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 055 990 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
29.11.2000 Bulletin 2000/48

(51) Int Cl.7: G06F 1/00

(21) Application number: 99304165.6

(22) Date of filing: 28.05.1999

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(71) Applicant: Hewlett-Packard Company
Palo Alto, California 94304-1112 (US)

(72) Inventors:
- Proudler, Graeme
Bristol BS34 8XQ (GB)
- Balacheff, Boris
Bristol BS31 2HJ (GB)
- Pearson, Siani
Bristol BS9 3PZ (GB)
- Chan, David
California CA 95030 (US)

(74) Representative: Lawman, Matthew John Mitchell
Hewlett-Packard Limited,
IP Section,
Building 3,
Filton Road
Stoke Gifford, Bristol BS34 8QZ (GB)

(54) Event logging in a computing platform

(57) There is disclosed a computer entity having a trusted component which compiles an event log for events occurring on a computer platform. The event log contains event data of types which are pre-specified by a user by inputting details through a dialogue display generated by the trusted component. Items which can be monitored include data files, applications drivers and the like. The trusted component operates through a monitoring agent which may be launched onto the computer platform. The monitoring agent may be periodically interrogated to make sure that it is operating correctly and responding to interrogations by the trusted component.

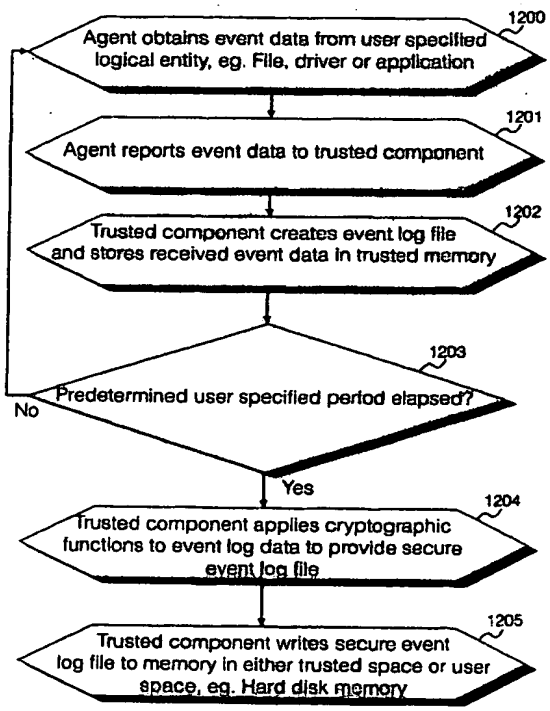

Fig. 12

EP 1 055 990 A1

form and the status of the data within the platform or system is dynamic and difficult to predict. It is difficult to determine whether a computer platform is operating correctly because the state of the computer platform and data on the platform is constantly changing and the computer platform itself may be dynamically changing.

- From a security point of view, commercial computer platforms, in particular client platforms, are often deployed in environments which are vulnerable to unauthorized modification. The main areas of vulnerability include modification by software loaded by a user, or by software loaded via a network connection. Particularly, but not exclusively, conventional computer platforms may be vulnerable to attack by virus programs, with varying degrees of hostility.

- Computer platforms may be upgraded or their capabilities extended or restricted by physical modification, i.e. addition or deletion of components such as hard disk drives, peripheral drivers and the like.

[0008] It is known to provide certain security features in computer systems, embedded in operating software. These security features are primarily aimed at providing division of information within a community of users of the system.

[0009] In the known Microsoft Windows NT™ 4.0 operating system, there also exists a monitoring facility called "system log event viewer" in which a log of events occurring within the platform is recorded into an event log data file which can be inspected by a system administrator using the windows NT operating system software. This facility goes someway to enabling a system administrator to security monitor pre-selected events. The event logging function in the Windows NT™ 4.0 operating system is an example of system monitoring.

[0010] However, in terms of overall security of a computer platform, a purely software based system is vulnerable to attack, for example by viruses. The Microsoft Windows NT™ 4.0 software includes a virus guard software, which is preset to look for known viruses. However, virus strains are developing continuously, and the virus guard software will not guard against unknown viruses.

[0011] Further, prior art monitoring systems for computer entities focus on network monitoring functions, where an administrator uses network management software to monitor performance of a plurality of network computers. Also, trust in the system does not reside at the level of individual trust of each hardware unit of computer platform in a system.

Summary of the Invention

[0012] Specific implementations of the present invention provide a computer platform having a trusted component which is physically and logically distinct from a computer platform. The trusted component has the properties of unforgability, and autonomy from the computer platform with which it is associated. The trusted component monitors the computer platform and thereby may provide a computer platform which is monitored on an individual basis at a level beneath a network monitoring or system monitoring level. Where a plurality of computer platforms are networked or included in the system, each computer platform may be provided with a separate corresponding respective trusted component.

[0013] Specific implementations of the present invention may provide a secure method of monitoring events occurring on a computer platform, in a manner which is incorruptible by alien agents present on the computer platform, or by users of the computer platform, in a manner such that if any corruption of the event log takes place, this is immediately apparent.

[0014] According to a first aspect of the present invention there is provided a computer entity comprising a computer platform comprising a data processor and at least one memory device; and a trusted component, said trusted component comprising a data processor and at least one memory device; wherein said data processor and said memory of said trusted component are physically and logically distinct from said data processor and memory of said computer platform; and means for monitoring a plurality of events occurring on said computer platform.

[0015] Preferably said monitoring means comprises a software agent operating on said computer platform, for monitoring at least one event occurring on said computer platform, and reporting said event to said trusted component.

[0016] Said software agent may comprise a set of program code normally resident in said memory device of said trusted component, said code being transferred into said computer platform for performing monitoring functions on said computer platform.

[0017] Preferably said trusted component comprises an event logging component for receiving data describing a plurality of events occurring on said computer platform, and compiling said event data into a secure event data.

[0018] Preferably said event logging component comprises means for applying a chaining function to said event data to produce said secure event data.

[0019] Selections of events and entities to be monitored may be selected by a user by operating a display interface for generating an interactive display comprising: means for selecting an entity of said computer platform to be monitored; and means for selecting at least one event to be monitored.

[0020] The monitoring means may further comprise prediction means for predicting a future value of at least one selected parameter.

Fig. 2 illustrates schematically connectivity of selected components of the computer entity of Fig. 1;

Fig. 3 illustrates schematically a hardware architecture of components of the computer entity of Fig. 1;

Fig. 4 illustrates schematically an architecture of a trusted component comprising the computer entity of Fig. 1;

Fig. 5 illustrates schematically a logical architecture of the computer entity, divided into a monitored user space, resident on the computer platform and a trusted space resident on the trusted component;

Fig. 6 illustrates schematically components of a monitoring agent which monitors events occurring on the computer platform and reports back to the trusted component;

Fig. 7 illustrates schematically logical components of the trusted component itself;

Fig. 8 illustrates schematically process steps carried out for establishing a secure communication between the user and the trusted component by way of a display on a monitor device;

Fig. 9 illustrates schematically process steps for selecting security monitoring functions using a display monitor;

Fig. 10 illustrates schematically a first dialogue box display generated by the trusted component;

Fig. 11 illustrates schematically a second dialogue box display used for entering data by a user;

Fig. 12 illustrates schematically operations carried out by the monitoring agent and the trusted component for monitoring logical and/or physical entities such as files, applications or drivers on the computer platform;

Fig. 13 illustrates schematically process steps operated by the agent and trusted component for continuous monitoring of specified events on the computer platform; and

Fig. 14 illustrates schematically process steps carried out by and interaction between the monitoring agent and the trusted component for implementing the agent on the computer platform, and monitoring the existence and integrity of the agent on the computer platform.

Detailed Description of the Best Mode for Carrying Out the Invention

[0035] There will now be described by way of example the best mode contemplated by the inventors for carrying out the invention. In the following description numerous specific details are set forth in order to provide a thorough understanding of the present invention. It will be apparent however, to one skilled in the art, that the present invention may be practiced without limitation to these specific details. In other instances, well known methods and structures have not been described in detail so as not to unnecessarily obscure the present invention.

[0036] In this specification, the term "trusted" when used in relation to a physical or logical component, is used to mean a physical or logical component with which the behavior of that component is predictable and known. Trusted components have a high degree of resistance to unauthorised modification.

[0037] In this specification, the term "computer platform" is used to refer to at least one data processor and at least one data storage means, usually but not essentially with associated communications facilities eg a plurality of drivers, associated applications and data files, and which may be capable of interacting with external entities eg. a user or another computer entity, for example by means of connection to the internet, connection to an external network, or by having an input port capable of receiving data stored on a data storage medium, eg a CD ROM, floppy disk, ribbon tape or the like. The term "computer platform" encompasses the main data processing and storage facility of a computer entity.

[0038] Referring to Fig. 1 herein, there is illustrated schematically one example of a computer entity as previously described in the applicant's European patent application entitled "Trusted Computing Platform", filed 15 February 1999 at the European Patent Office a copy of which is filed herewith, and the entire contents of which are incorporated herein by reference. Referring to Fig. 2 of the accompanying drawings, there is illustrated schematically physical connectivity of some of the components of the trusted computer entity of Fig. 1. Referring to Fig. 3 herein, there is illustrated schematically an architecture of the trusted computer entity of Figs. 1 and 2, showing physical connectivity of components of the entity.

[0039] In general, in the best mode described herein, a trusted computer entity comprises a computer platform consisting of a first data processor, and a first memory means, together with a trusted component which verifies the integrity and correct functioning of the computing platform. The trusted component comprises a second data processor and a second memory means, which are physically and logically distinct from the first data processor and first memory means.

[0040] In the example shown in Figs. 1 to 3 herein, the trusted computer entity is shown in the form of a per-

image data may comprise a photograph of a user. The image data on the smart card may be unique to a person using the smart card.

[0050] In the best mode herein, a user may specify a selected logical or physical entity on the computer platform, for example a file, application, driver, port, interface or the like for monitoring of events which occur on that entity. Two types of monitoring may be provided, firstly continuous monitoring over a predetermined period, which is set by a user through the trusted component, and secondly, monitoring for specific events which occur on an entity. In particular, a user may specify a particular file of high value, or of restricted information content and apply monitoring of that specified file so that any interactions involving that file, whether authorized or not, are automatically logged and stored in a manner in which the events occurring on the file cannot be deleted, erased or corrupted, without this being immediately apparent.

[0051] Referring to Fig. 4 herein, there is illustrated schematically an internal architecture of trusted component 202. The trusted component comprises a processor 400, a volatile memory area 401; a non-volatile memory area 402; a memory area storing native code 403; and a memory area storing one or a plurality of cryptographic functions, 404, the non-volatile memory 401, native code memory 403 and cryptographic memory 404 collectively comprising the second memory means hereinbefore referred to.

[0052] Trusted component 202 comprises a physically and logically independent computing entity from the computer platform. In the best mode herein, the trusted component shares a motherboard with the computer platform so that the trusted component is physically linked to the computer platform. In the best mode, the trusted component is physically distinct from the computer platform, that is to say it does not exist solely as a sub-functionality of the data processor and memory means comprising the computer platform, but exists separately as a separate physical data processor 400 and separate physical memory area 401, 402, 403, 404. By providing a physically present trusted component, the trusted component becomes harder to mimic or forge through software introduced onto the computer platform. Programs within the trusted component are pre-loaded at manufacture of the trusted component, and are not user configurable. The physicality of the trusted component, and the fact that the user component is not configurable by the user enables the user to have confidence in the inherent integrity of the trusted component, and therefore a high degree of "trust" in the operation and presence of the trusted component on the computer platform.

[0053] Referring to Fig. 5 herein, there is illustrated schematically a logical architecture of the computer entity 500. The logical architecture has a same basic division between the computer platform, and the trusted component, as is present with the physical architecture described in Figs. 1 to 3 herein. That is to say, the trusted component is logically distinct from the computer platform to which it is physically related. The computer entity comprises a user space 504 being a logical space which is physically resident on the computer platform (the first processor and first data storage means) and a trusted component space 513 being a logical space which is physically resident on the trusted component 202. In the user space 504 are one or a plurality of drivers 506, one or a plurality of applications programs 507, a file storage area 508; smart card reader 108; smart card interface 305; and a software agent 511 which operates to perform operations in the user space and report back to trusted component 202. The trusted component space is a logical area based upon and physically resident in the trusted component, supported by the second data processor and second memory area of the trusted component. Confirmation key device 104 inputs directly to the trusted component space 513, and monitor 100 receives images directly from the trusted component space 513. External to the computer entity are external communications networks eg the Internet 501, and various local area networks, wide area networks 502 which are connected to the user space via the drivers 506 which may include one or more modem ports. External user smart card 503 inputs into smart card reader 108 in the user space.

[0054] In the trusted component space, are resident the trusted component itself, displays generated by the trusted component on monitor 100; and confirmation key 104, inputting a confirmation signal via confirmation key interface 306.

[0055] Referring to Fig. 6 herein, within agent 511, there is provided a communications component 601 for communicating with the trusted component 202; and a file monitoring component 600 the purpose of which is to monitor events occurring on specified logical or physical entities, eg data files, applications or drivers on the computer platform, within the user space.

[0056] Referring to Fig. 7 herein, there is illustrated schematically internal components on the trusted component 202 resident in trusted space 513. The trusted component comprises a communications component 700 for communicating with software agent 511 in user space; a display interface component 701 which includes a display generator for generating a plurality of interface displays which are displayed on monitor 100 and interface code enabling a user of the computing entity to interact with trusted component 202; an event logger program 702 for selecting an individual file, application, driver or the like on the computer platform, and monitor the file, application or driver and compile a log of events which occur on the file, application or driver; a plurality of cryptographic functions 703 which are used to cryptographically link the event log produced by event logger component 702 in a manner from which it is immediately apparent if the event log has been tampered with after leaving event logger 702; a set of prediction

described primarily in relation to data files, application programs and drivers, although it will be appreciated that the general methods and principles described herein are applicable to the general set of components and facilities of the computer platform. By activating the drop down menu on each of selection boxes 1101-1103, there is listed a corresponding respective list of data files, drivers, or applications which are present on the computer platform. A user may select any of these files and/or applications and/or drivers by activating the pointing device on the selected icon from the drop down menu in conventional manner in steps 904, 905, 906. Additionally, the event monitor menu comprises an event select menu 1104. The event select menu lists a plurality of event types which can be monitored by the event logger 702 within the trusted component, for the file, application or driver which is selected in selection boxes 1101, 1102, 1103 respectively. Types of event which can be monitored include events in the set: file copied - the event of a selected file being copied by an application or user; file saved - the event of whether a specified file is saved by an application or user; file renamed - the event of whether a file has been renamed by an application or user; file opened - the event of whether a file is opened by an application or user; file overwritten - the event of whether data within a file has been overwritten; file read - the event of whether data in a file has been read by any user, application or other entity; file modified - the event of whether data in a file has been modified by a user, application or other entity; file printed - the event of whether a file has been sent to a print port of the computer entity; driver used - whether a particular driver has been used by any application or file; driver reconfigured - the event of whether a driver has been reconfigured; modem used - subset of the driver used event, applying to whether a modem has been used or not; disk drive used - the event of whether a disk drive has been used in any way, either written or read; application opened - the event of whether an application has been opened; and application closed - the event of whether an application has been closed. Once the user has selected the application, driver or file and the events to be monitored in dialog box 1100, the user activates the confirmation key 104, which is confirmed by confirmation key icon 1105 visually altering, in order to activate a monitoring session. A monitoring session can only be activated by use of the dialog box 1100, having the user's image 1001 from the user's smart card display thereon, and by independently pressing confirmation key 104. Display of the image 1001 on the monitor 100, enables the user to have confidence that the trusted component is generating the dialog box. Pressing the confirmation key 104 by the user, which is directly input into trusted component 202 independently of the computer platform gives direct confirmation to the trusted component that the user, and not some other entity, e. g. a virus or the like is activating the monitoring session.

[0061] The user may also specify a monitoring period by entering a start time and date and a stop time and date in data entry window 1106. Alternatively, where a single event on a specified entity is to be monitored, the user can specify monitoring of that event only by confirming with pointing device 105 in first event only selection box 1107.

[0062] Two modes of operation will now be described, in the first mode of operation, continuous event monitoring of specified entities over a user specified period occurs. In the second mode of operation, continuous monitoring of a specified entity occurs until a user specified event has happened, or until a user specified period for monitoring that user specified event has elapsed.

[0063] In Fig. 12 herein, there is illustrated a procedure for continuous monitoring of a specified logical or physical entity over a user specified monitoring period.

[0064] Referring to Fig. 12 herein, there is illustrated schematically process steps operated by trusted component 202 in response to a user input to start an event monitoring session as described with reference to figs. 8 to 11 herein before. In step 1200, display interface 701 receives commands from the user via the dialogue boxes which are input using pointing device 105, keyboard 101 via data bus 304 and via communications interface 700 of the trusted component. The event logger 702 instructs agent 511 in user space to commence event monitoring. The instructions comprising event logger 702 are stored within a memory area resident within the trusted component 202. Additionally, event logger 702 is also executed within a memory area in the trusted component. In contrast, whilst the instructions comprising agent 511 are stored inside the trusted components 202 in a form suitable for execution on the host processor ie in CPU native programs area 403 of the trust component, agent 511 is executed within untrusted user space ie outside of the trusted component 202. Agent 511 receives details of the file, application and/or drivers to be monitored from event logger 702. In step 1200, agent 511 receives a series of event data from the logical entity (eg file, application or driver) specified. Such monitoring is a continuous process, and agent 511 may perform step 1200 by periodically reading a data file in which such event data is automatically stored by the operating system (for example in the Microsoft windows 4.0™ operating system which contains the facility for logging events on a file). However, in order to maximize security, it is preferable the agent 511 periodically gathers event data itself by interrogating the file, application or driver directly to elicit a response. In step 1201, the collected data concerning the events of entity are reported directly to the trusted component 202, which then stores them in a trusted memory area in step 1202. In step 1203, the event logger checks whether the user specified predetermined monitoring period from the start of the event monitoring session has elapsed. If the event monitoring session period has not yet elapsed, event logger 702 continues to await further events on the specified files, applications or drivers supported by

dressed; a network address to which a file has been copied, to which an application has addressed, or to which a driver has corresponded with.

[0072] The event data stored in the event log may be physically stored in a data file either on the platform or in the trusted component. The event log data is secured using a chaining function, such that a first secured event data is used to secure a second secured event data, a second secured event data is used to secure a third event data, etc so any changes to the chain of data are apparent.

[0073] In addition to providing the secured event log data, the trusted component may also compile a report of events. The report may be displayed on monitor 100. Items which may form the content of a report include the events as specified in the event log above, together with the following: time of an event, date of an event, whether or not a password was used, a destination of the file it is copied to, a size of a file (in megabytes), a duration a file or application has been open, a duration over which a driver has been online, a duration over which a driver has been used, a port which has been used, an internet address which has been communicated with, a network address which has been communicated with.

[0074] Agent 511 performs event monitoring operations on behalf of trusted component 202, however whereas trusted component 202 is resident in a trusted space 513, agent 511 must operate in the user space of the computer platform. Because the agent 511 is in an inherently less secure environment than the trusted space 513, there is the possibility that agent 511 may become compromised by hostile attack to the computer platform through a virus or the like. The trusted component deals with the possibility of such hostile attack by either of two mechanisms. Firstly, in an alternative embodiment the agent 511 may be solely resident within trusted component 202. All operations performed by agent 511 are performed from within trusted user space 513 by the monitoring code component 600 operating through the trusted components' communications interface 700 to collect event data. However, a disadvantage of this approach is that since agent 511 does not exist, it cannot act as a buffer between trusted component 202 and the remaining user space 504.

[0075] On the other hand, the code comprising agent 511 can be stored within trusted space in a trusted memory area of trusted component 202, and periodically "launched" into user space 504. That is to say, when a monitoring session is to begin, the agent can be downloaded from the trusted component into the user space or kernel space on the computer platform, where it then resides, performing its continuous monitoring functions. In this second method, which is the best mode contemplated by the inventors, to reduce the risk of any compromises of agent 511 remaining undetected, the trusted component can either re-launch the complete agent from the secure memory area in trusted space into the user space at periodic intervals, and/or can periodically monitor the agent 511 in user space to make sure that it is responding correctly to periodic interrogation by the trusted component.

[0076] Where the agent 511 is launched into user space from its permanent residence in trusted space, this is effected by copying code comprising the agent from the trusted component onto the computer platform. Where a monitoring session has a finite monitoring period specified by a user, the period over which the agent 511 exists in user space can be configured to coincide with the period of the monitoring session. That is to say the agent exists for the duration of the monitoring session only, and once the monitoring session is over, the agent can be deleted from user/kernel space. To start a new monitoring session for a new set of events and/or entities, a new agent can be launched into user space for the duration of that monitoring session.

[0077] During the monitoring session, which may extend over a prolonged period of days or months as specified by a user, the trusted component monitors the agent itself periodically.

[0078] Referring to Fig. 14 herein, there is illustrated schematically process steps carried out by trusted component 202 and agent 511 on the computer platform for launching the agent 511 which is downloaded from trusted space to user space, and in which the trusted component monitors the agent 511 once set up and running on the computer platform.

[0079] In step 1400, native code comprising the agent 511 stored in the trusted components secure memory area is downloaded onto the computer platform by the computer platform reading the agent code directly from the trusted component in step 1401. In step 1402, the data processor on the computer platform commences execution of the native agent code resident in user space on the computer platform. The agent continues to operate as described herein before continuously in step 1403. Meanwhile, trusted component 202 generates a nonce challenge message in step 1404 after a suitable selected interval, and sends this nonce to the agent which receives it in step 1405. The nonce may comprise a random bit sequence generated by the trusted component. The purpose of the nonce is to allow the trusted component to check that the agent is still there and is still operating. If the nonce is not returned by the agent, then the trusted component knows that the agent has ceased to operate and/or has been compromised. In step 1407 the agent signs the nonce and in step 1408 the agent sends the signed nonce back to the trusted component. The trusted component receives the signed nonce in step 1409 and then repeats step 1404 sending a new nonce after a pre-selected period. If after a predetermined wait period 1406, commencing when the nonce was sent to the agent in step 1404, the trusted component has not received a nonce returned from the agent, then in step 1410 the trusted component generates an alarm signal which may result in a display on the monitor showing that the agent 511 is incorrectly op-

compiling said event data into secure event data.

5. The computer entity as claimed in claim 4, wherein said event logging component comprises means for applying a chaining function to said event data to produce said secure event data.

6. The computer entity as claimed in claim 1, further comprising a display interface for generating an interactive display comprising:

means for selecting an entity of said computer platform to be monitored; and

means for selecting at least one event to be monitored.

7. The computer entity as claimed in claim 1, further comprising prediction means for predicting a future value of at least one selected parameter.

8. The computer entity as claimed in claim 1, further comprising a confirmation key means connected to said trusted component, and independent of said computer platform, for confirming to said trusted component an authorisation signal of a user.

9. The computer entity as claimed in claim 1, wherein logical entities to be monitored are selected from the set:

at least one data file;

at least one application;

at least one driver component.

10. A computer entity comprising:

a computer platform having a first data processor and a first memory device; and

a trusted monitoring component comprising a second data processor and a second memory device, wherein

said trusted monitoring component stores an agent program resident in said second memory area, said agent program arranged to be copied to said first memory area for performing functions on behalf of said trusted component, under control of said first data processor.

11. A computer entity comprising:

a computer platform comprising a first data processor and a first memory device;

a trusted monitoring component comprising a second data processor and a second memory device;

a first computer program resident in said first memory area and operating said first data processor, said first computer program reporting back events concerning operation of said computer platform to said trusted monitoring component; and

a second computer program said second computer program resident in said second memory area of said trusted component, said second program operating to monitor an integrity of said first program.

12. The computer entity as claimed in claim 11, wherein said computer program monitors an integrity of said first computer program by sending to said first computer program a plurality of interrogation messages, and monitoring a reply to said interrogation messages made by said first computer program.

13. The computer entity as claimed in claim 12, wherein a said interrogation message is sent in a first format, and returned in a second format, wherein said second format is a secure format.

14. A method of monitoring a computer platform comprising a first data processor and a first memory means, said method comprising the steps of:

reading event data describing events occurring on at least one logical or physical entity comprising said computer platform;

securing said event data in a second data processing means having an associated second memory area, said second data processing means, said second memory area being physically and logically distinct from said first data processing means and said first memory area, such that said secure event data cannot be altered without such alteration being apparent.

15. The method as claimed in claim 14, where a said event to be monitored is selected from the set of events:

copying of a data file;

saving a data file;

renaming a data file;

opening a data file;

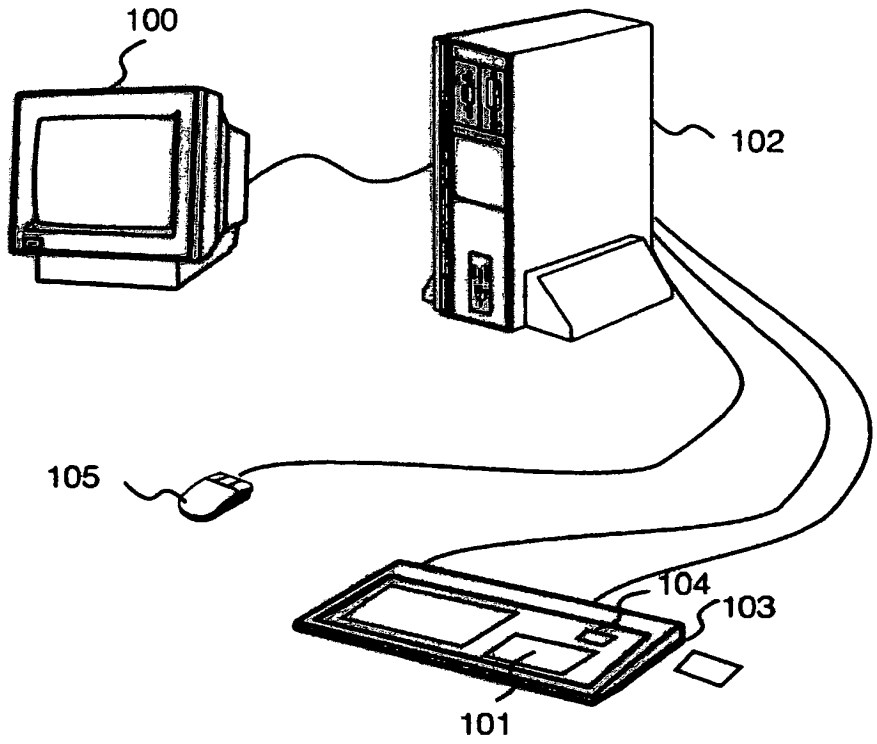

Fig. 1

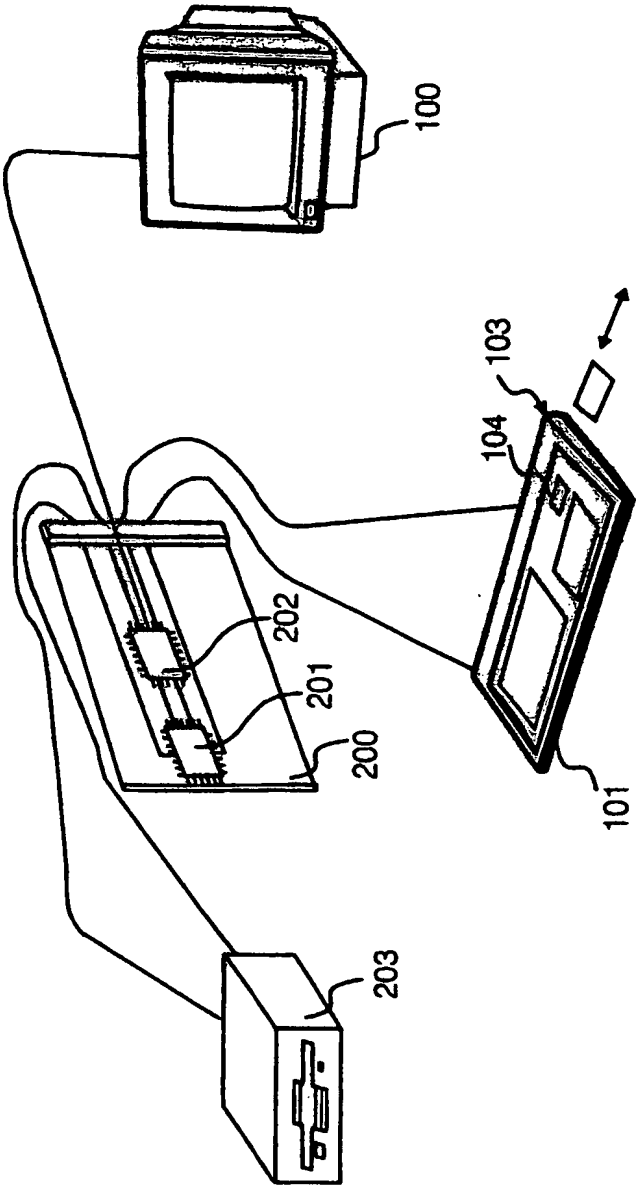

Fig. 2

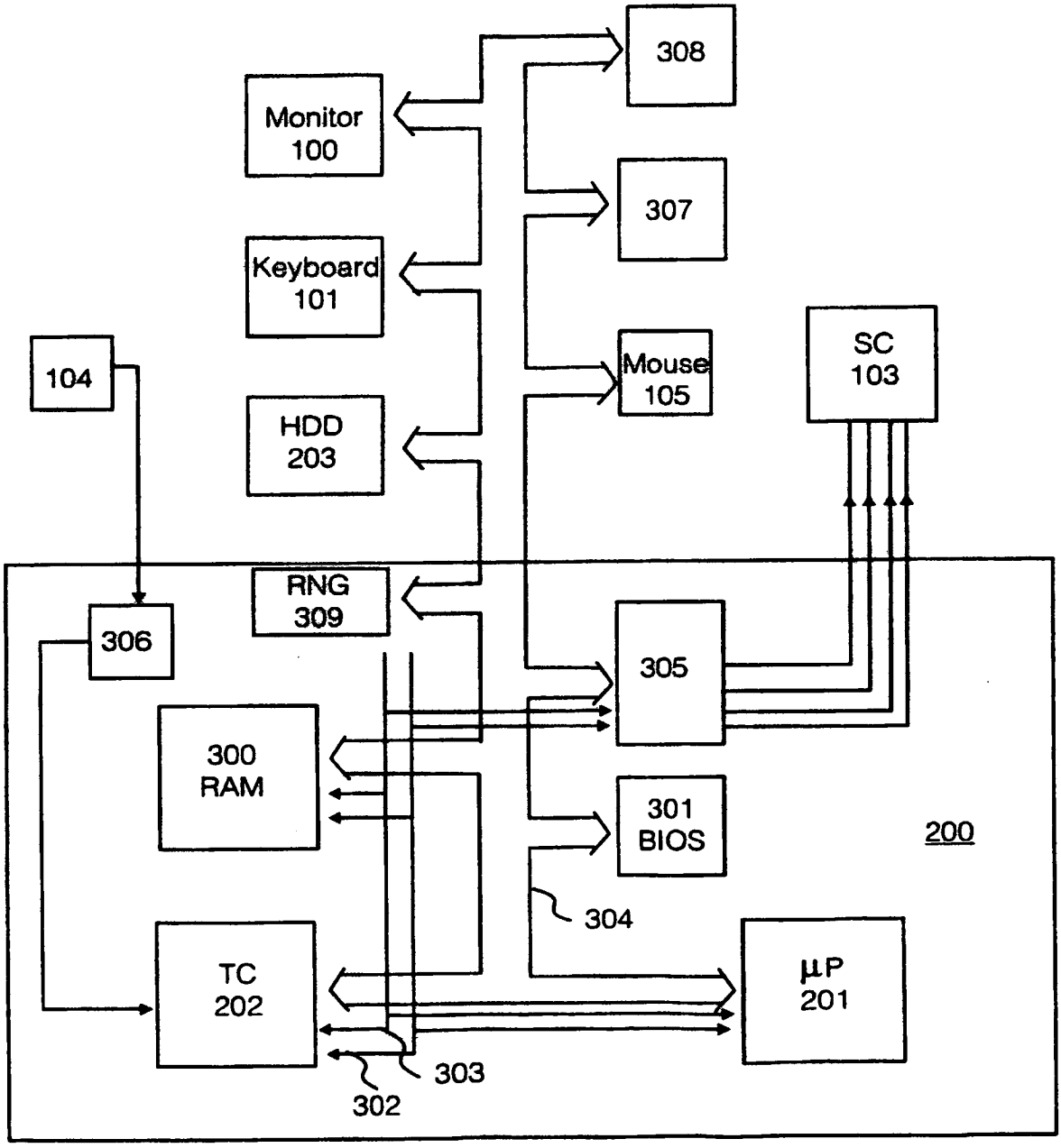
308
Monitor
100
307
Keyboard
101
SC
103
104
Mouse
105
HDD
203
RNG
309
306
305
300
RAM
301
BIOS
200
304
TC
202
µP
201
303
302

Fig. 3

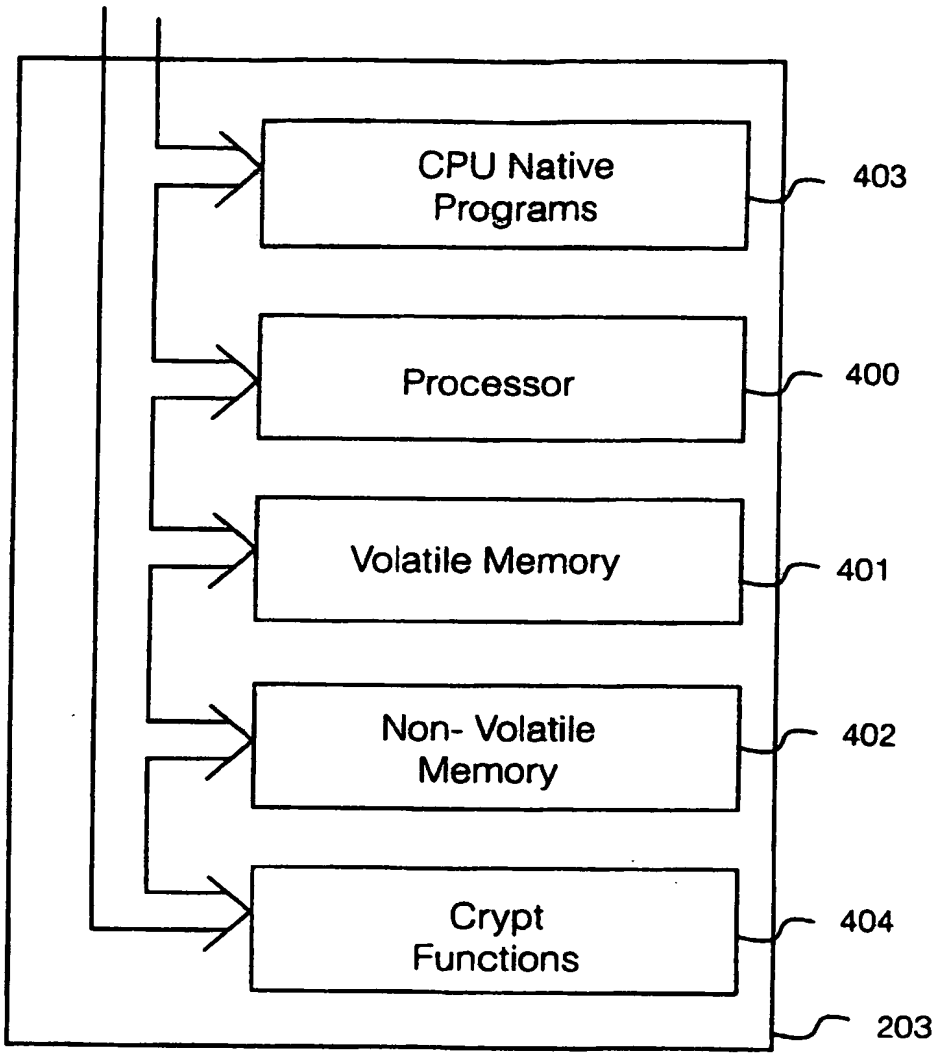
CPU Native Programs
403
Processor
400
Volatile Memory
401
Non- Volatile Memory
402
Crypt Functions
404
203

Fig. 4

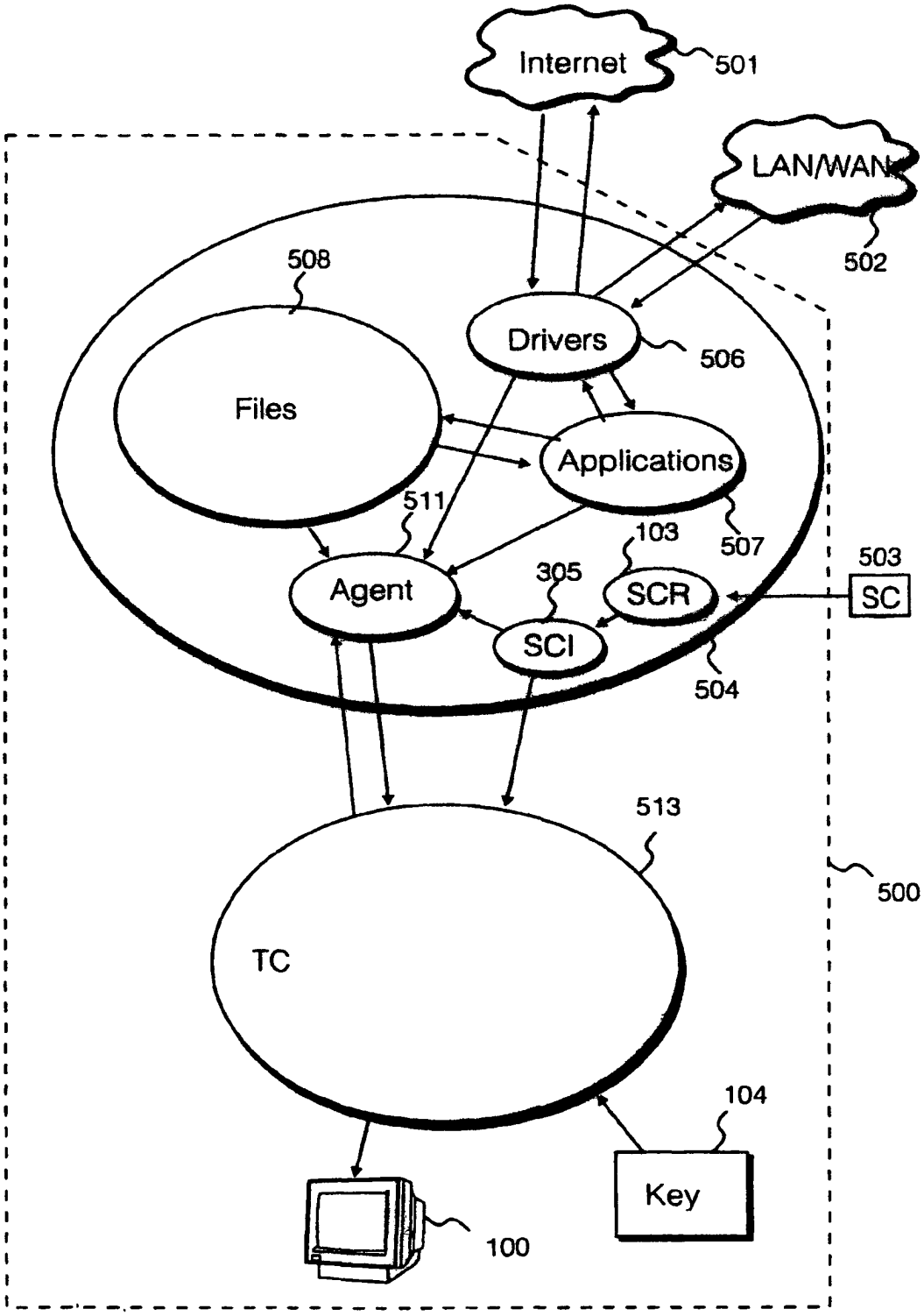
Internet
501
LAN/WAN
502
508
Drivers
506
Files
Applications
511
103
507
503
305
SCR
SC
Agent
SCI
504
513
500
TC
104
Key
100

Fig. 5

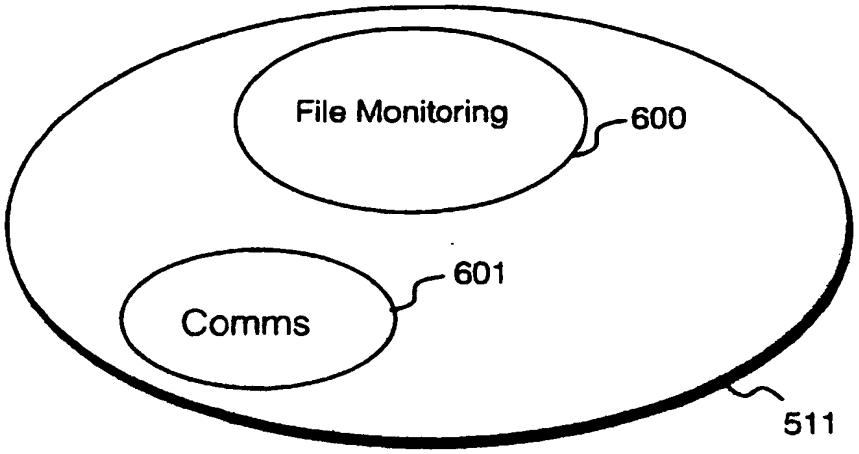

Fig. 6

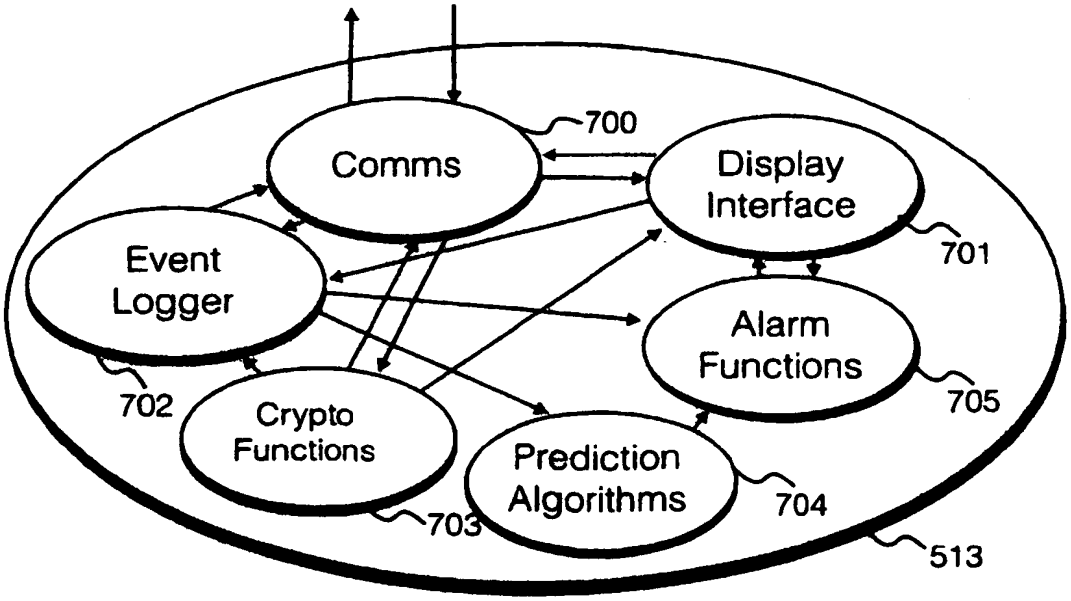

Fig. 7

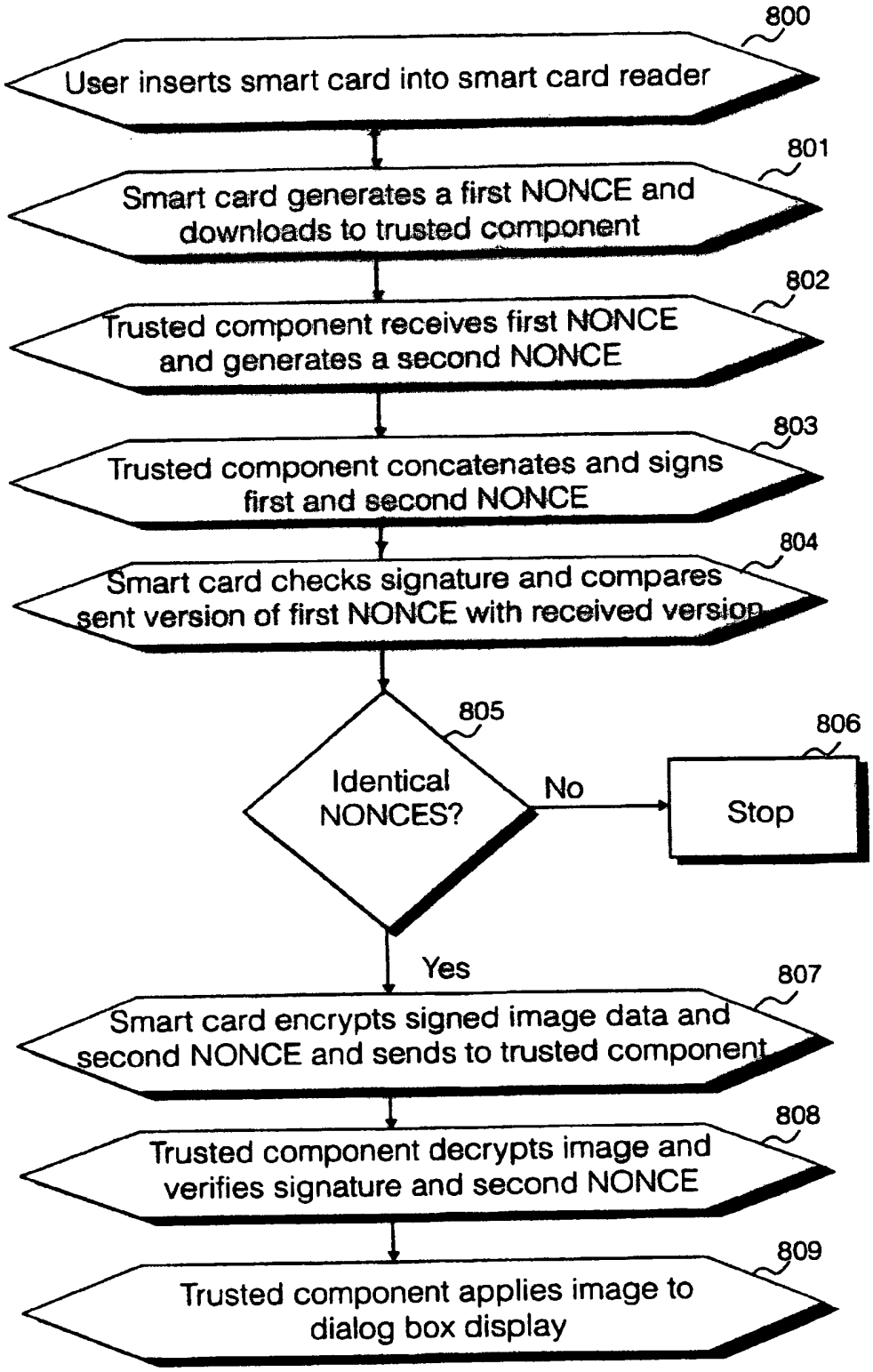
800
User inserts smart card into smart card reader
801
Smart card generates a first NONCE and downloads to trusted component
802
Trusted component receives first NONCE and generates a second NONCE
803
Trusted component concatenates and signs first and second NONCE
804
Smart card checks signature and compares sent version of first NONCE with received version
805
Identical NONCES?
No
806
Stop
Yes
807
Smart card encrypts signed image data and second NONCE and sends to trusted component
808
Trusted component decrypts image and verifies signature and second NONCE
809
Trusted component applies image to dialog box display

Fig. 8

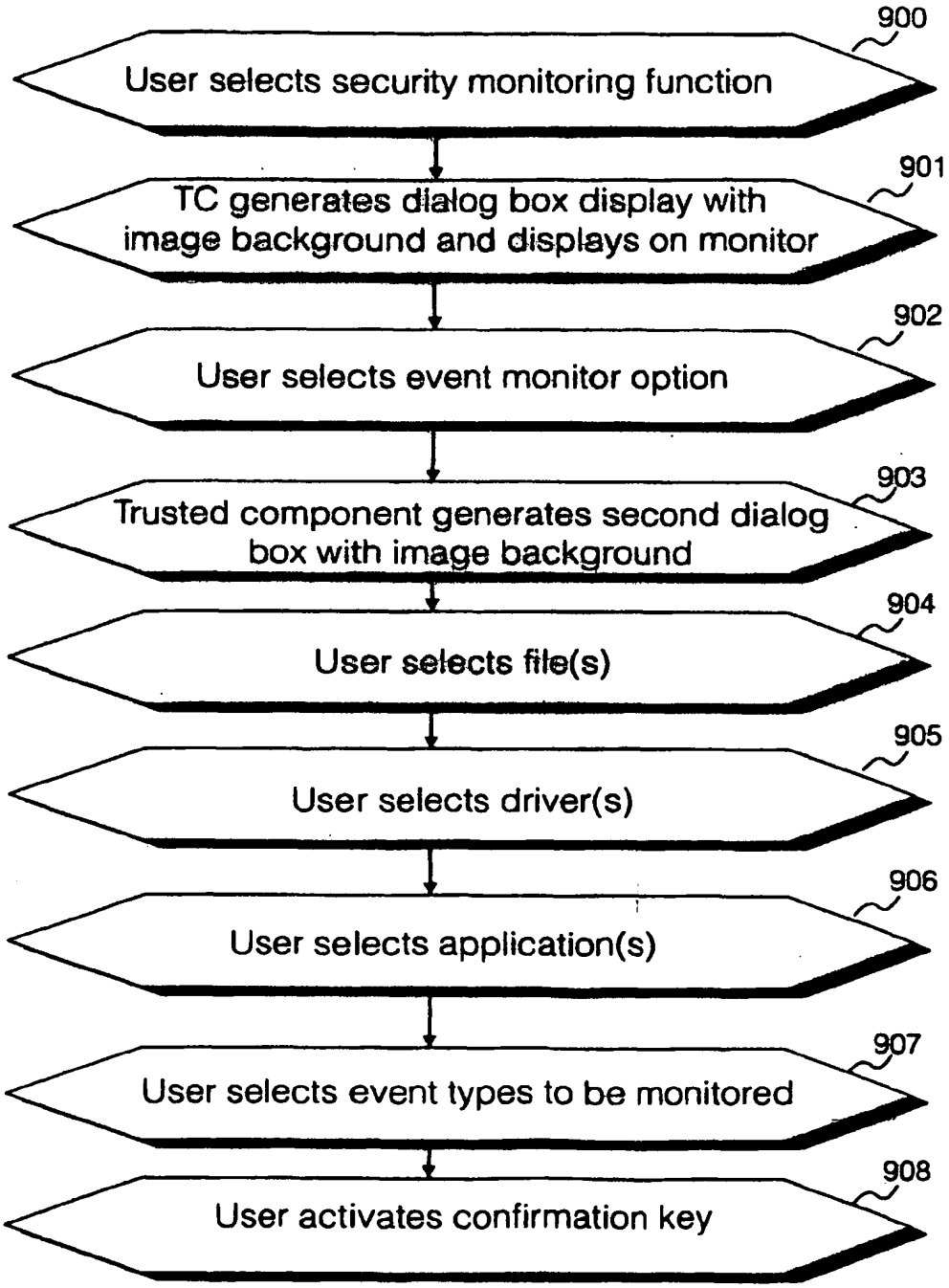
900
User selects security monitoring function
901
TC generates dialog box display with image background and displays on monitor
902
User selects event monitor option
903
Trusted component generates second dialog box with image background
904
User selects file(s)
905
User selects driver(s)
906
User selects application(s)
907
User selects event types to be monitored
908
User activates confirmation key

Fig. 9

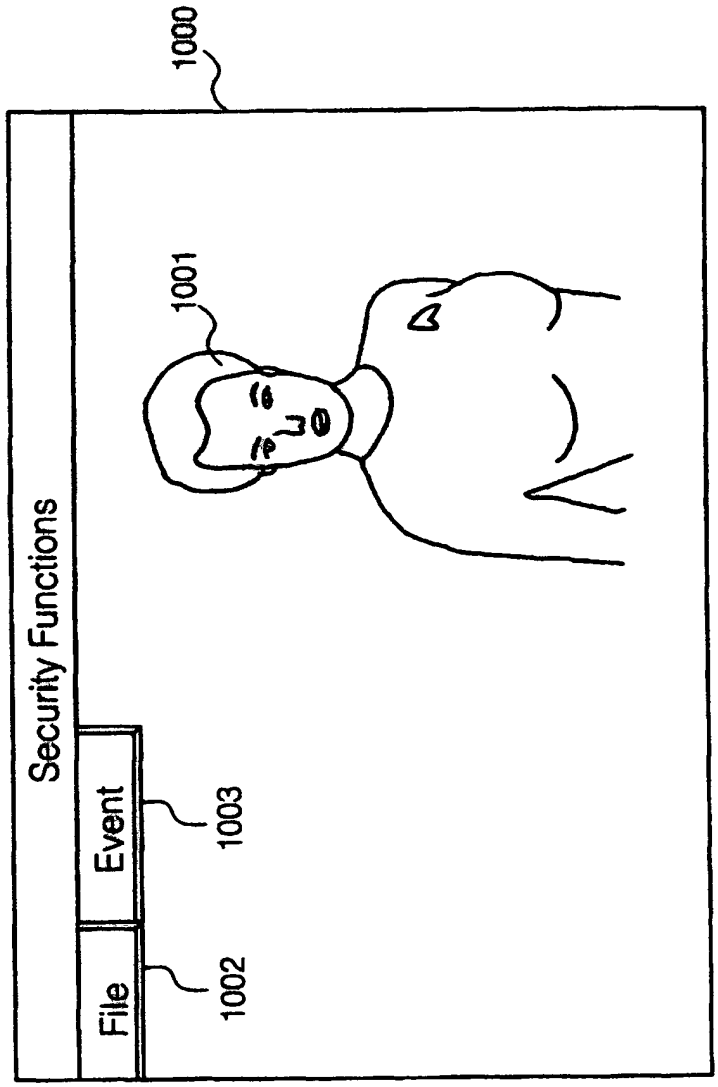

Fig. 10

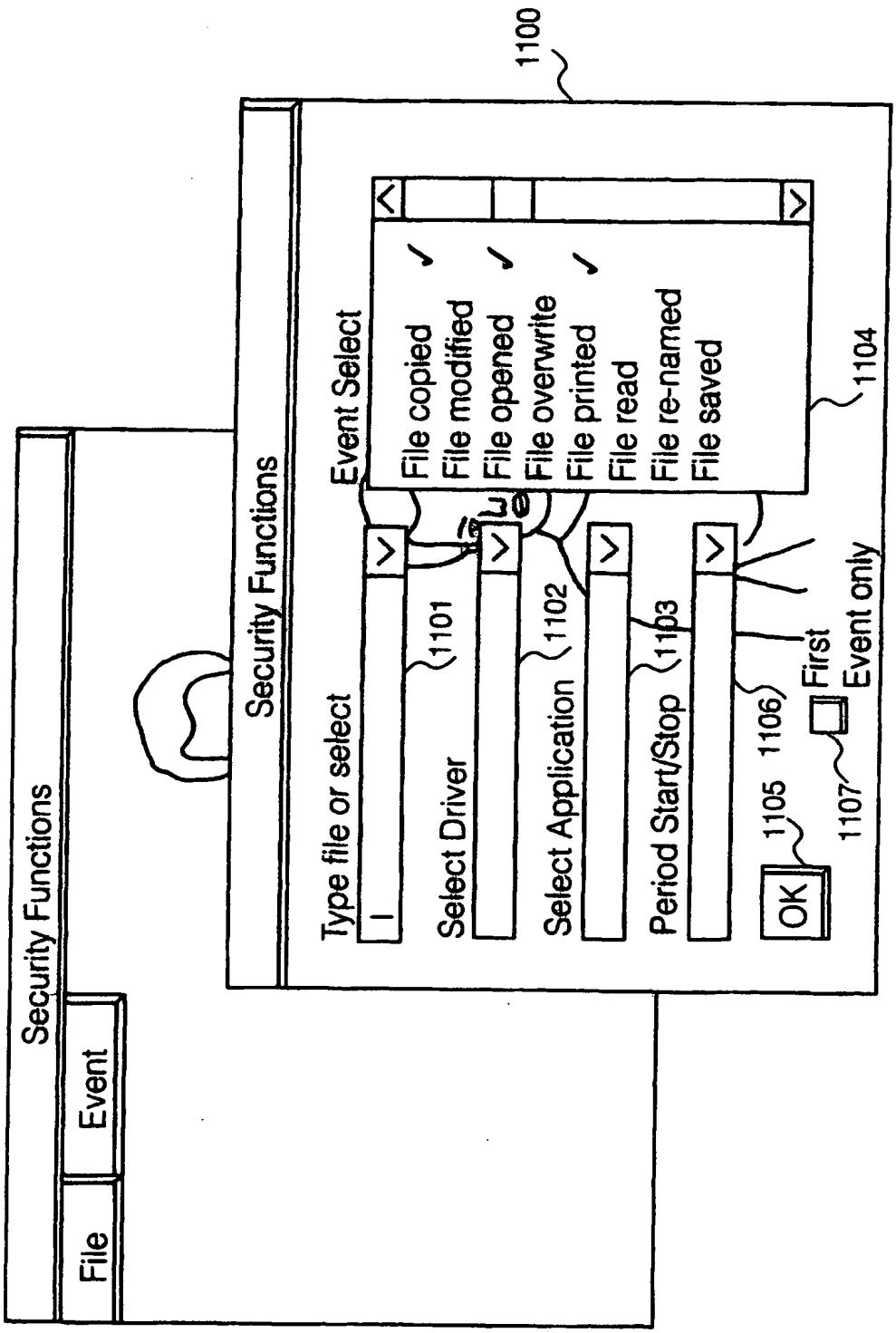
1100
Security Functions
Event
File
Security Functions
Event Select
File copied
File modified
File opened
File overwrite
File printed
File read
File re-named
File saved
1104
Type file or select
1101
Select Driver
1102
Select Application
1103
Period Start/Stop
1105
OK
1106
First
Event only
1107

Fig. 11

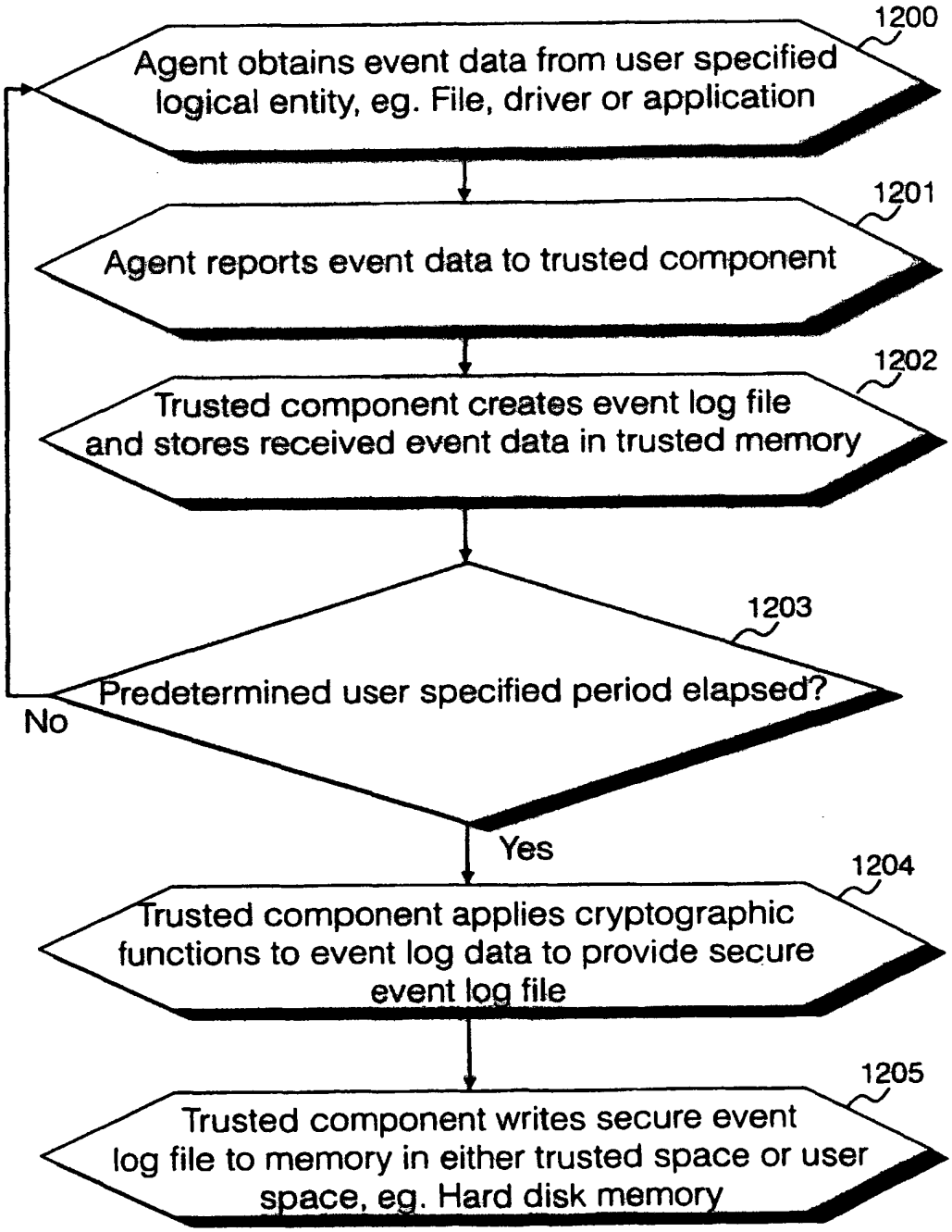
1200
Agent obtains event data from user specified logical entity, eg. File, driver or application
1201
Agent reports event data to trusted component
1202
Trusted component creates event log file and stores received event data in trusted memory
1203
Predetermined user specified period elapsed?
No
Yes
1204
Trusted component applies cryptographic functions to event log data to provide secure event log file
1205
Trusted component writes secure event log file to memory in either trusted space or user space, eg. Hard disk memory

Fig. 12

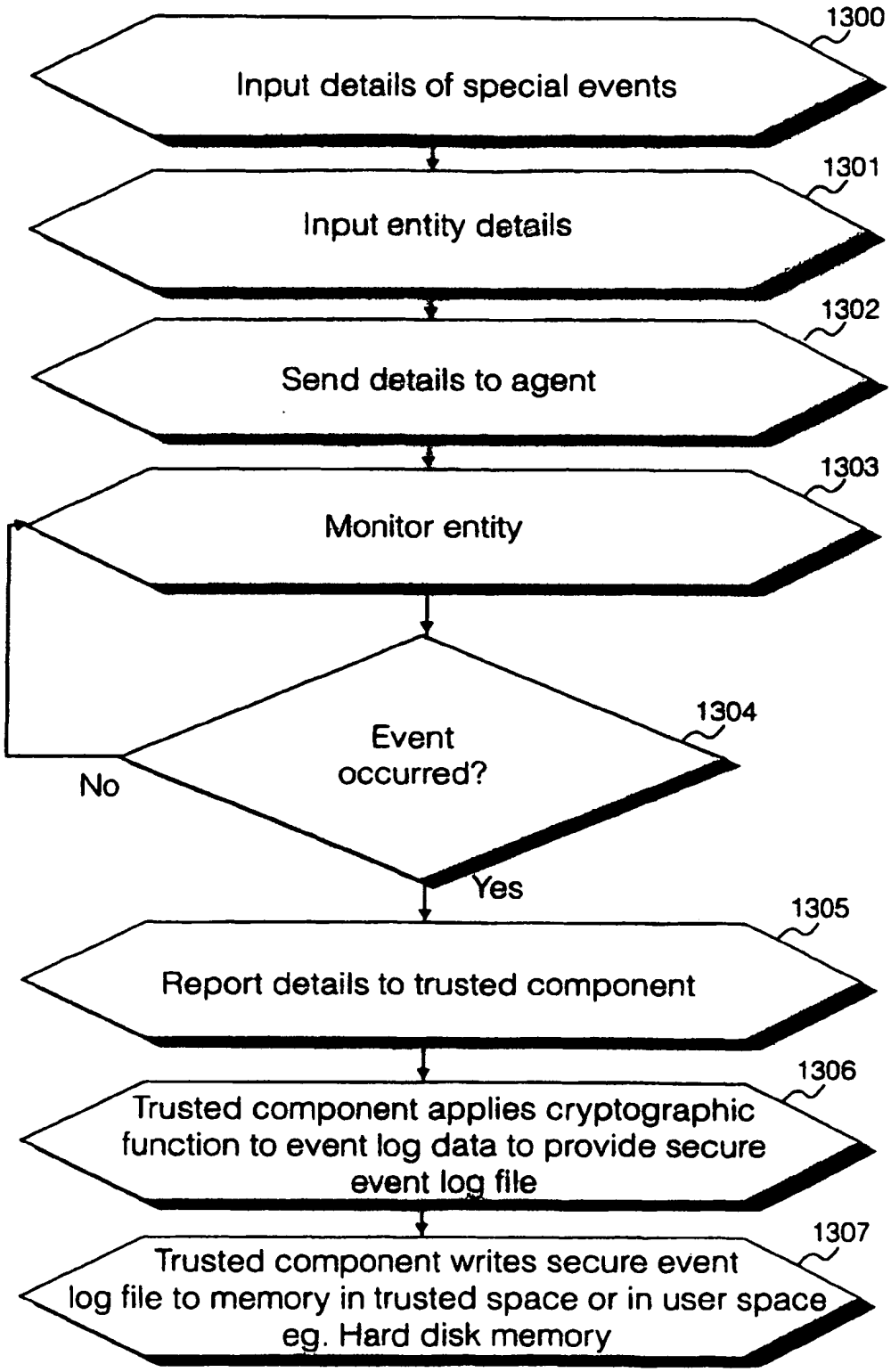
1300
Input details of special events
1301
Input entity details
1302
Send details to agent
1303
Monitor entity
1304
Event occurred?
No
Yes
1305
Report details to trusted component
1306
Trusted component applies cryptographic function to event log data to provide secure event log file
1307
Trusted component writes secure event log file to memory in trusted space or in user space eg. Hard disk memory

Fig. 13

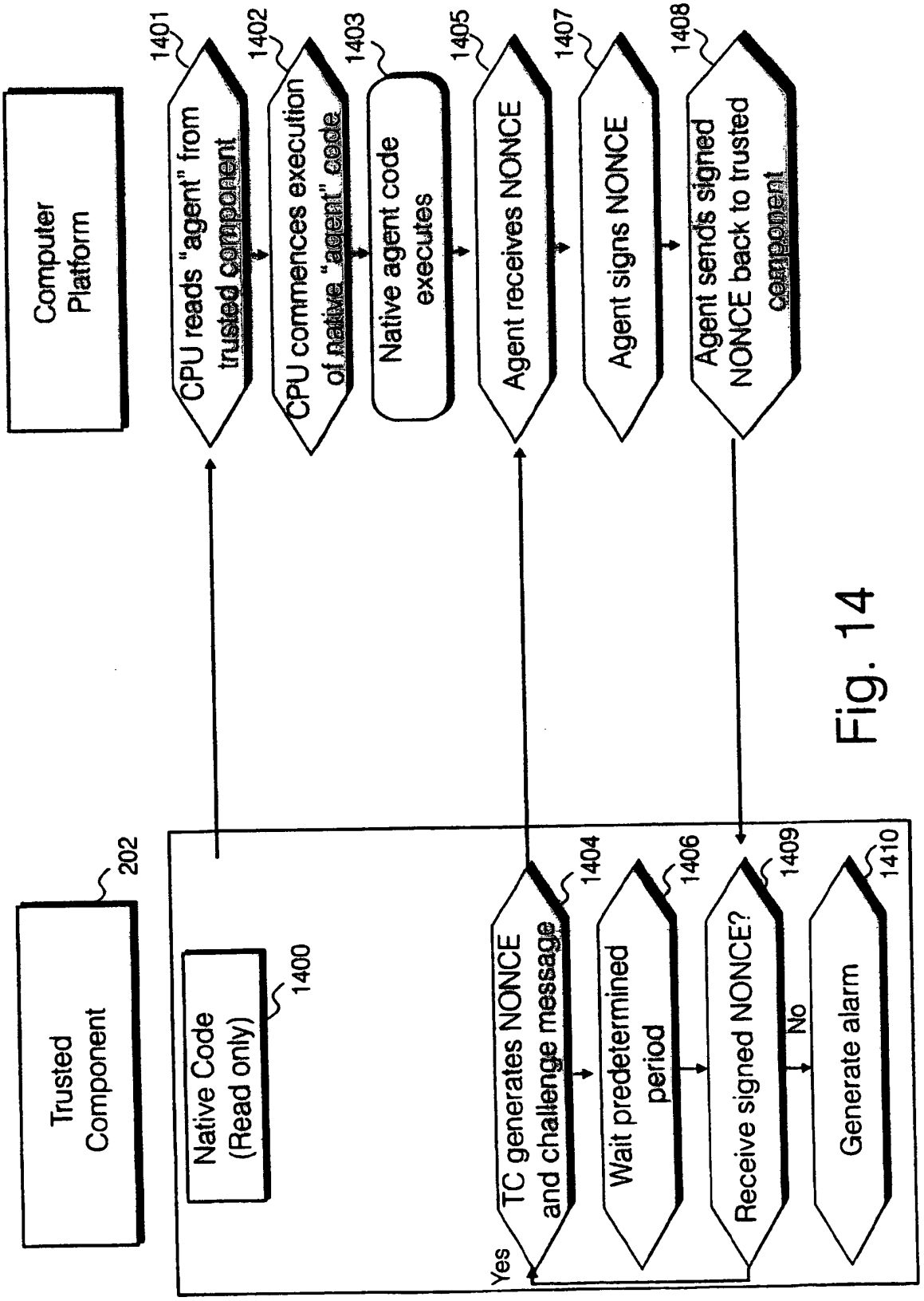
Computer Platform
1401
CPU reads "agent" from trusted component
1402
CPU commences execution of native "agent" code
1403
Native agent code executes
1405
Agent receives NONCE
1407
Agent signs NONCE
1408
Agent sends signed NONCE back to trusted component
Trusted Component
202
Native Code (Read only)
1400
TC generates NONCE and challenge message
1404
Wait predetermined period
1406
Receive signed NONCE?
1409
No
Yes
Generate alarm
1410

Fig. 14

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 99 30 4165

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
X	WO 98 45778 A (ZUTA MARC) 15 October 1998 (1998-10-15) * abstract; figure 1 * * page 16, line 1 - page 20, last line * * page 26, line 1 - page 32, last line *	1,14-16	G06F1/00
Y		2,3,10, 11,17-22	
Y	US 5 404 532 A (ALLEN WADE C ET AL) 4 April 1995 (1995-04-04) * the whole document *	2,3,10, 11	
Y	WO 95 27249 A (INTEL CORP) 12 October 1995 (1995-10-12) * abstract; figure 1 * * claims 1-36 *	17-19	
Y	CA 2 187 855 A (COMPONENT ORIENTED PROTECTIVE) 13 June 1997 (1997-06-13) * abstract; figure 1 * * claims 1-20 * * page 9, line 23 - page 10, last line *	20	
Y	WO 95 24696 A (INTEGRATED TECH AMERICA ;MOONEY DAVID M (US); WOOD DAVID E (US); K) 14 September 1995 (1995-09-14) * abstract; figure 3 * * page 2, line 26 - page 3, line 19 * * claims 1-20 *	21	
Y	EP 0 895 148 A (SIEMENS AG) 3 February 1999 (1999-02-03) * the whole document *	22	

TECHNICAL FIELDS SEARCHED (Int.Cl.7)
G06F

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	17 March 2000	Powell, D

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)